bitwarden | Help Center Article

PASSWORD MANAGER

Password Manager Overview

View in the help center:
https://bitwarden.com/help/password-manager-overview/

Password Manager Overview

Bitwarden Password Manager enables businesses and individuals to protect their online data in the face of rising cybercrime threats. Use Bitwarden Password Manager to generate strong, unique passwords for every account you use online. This way if one site suffers a data breach, none of your other accounts are compromised. Password Manager makes it easy to do this by creating, saving, and autofilling those strong passwords, so that you don't need to worry about remembering them.

Key features

For individuals and end-users, some of the most popular features that Bitwarden Password Manager offers are:

- **Easy import:** Import your credentials from almost any password management solution.
- **Robust autofill**: Use Password Manager to more easily log in to websites from browser extensions and from mobile apps.
- **Credential generators**: Use the username and password generator to confidently create secure credentials when signing up for new websites.
- **Integrated authentication**: Generate and autofill temporary one-time passwords (TOTP) for two-factor authentication (2FA) right from Bitwarden Password Manager.
- **Two-step login options**: Setup a variety of two-step login methods, including free options, to keep your important credentials secure.

For businesses and administrators, some of the most popular features that Bitwarden Password Manager offers are:

- **Easy import**: Import your company's shared credentials from almost any password management solution.
- **User management integrations**: Sync end-users to your Bitwarden organization using one of many system for cross-domain identity management (SCIM) or direct-to-directory integrations.
- **Login with SSO**: Authenticate your end-users with your existing single sign-on (SSO) setup through any SAML 2.0 or OIDC identity provider.
- **Robust policies**: Enforce security practices for your end-users, like setting up the ability for admins to recover lost accounts, using enterprise policies.

Security-first principles

Bitwarden is committed to building security-first products. Password Manager is:

- **Open source**: All source code is hosted on GitHub and is free for anyone to review and audit. Third-party auditing firms and security researchers are paid to do so regularly.
- **End-to-end encrypted**: All encryption and decryption of vault data is done client-side, meaning no sensitive data ever hits our servers unencrypted.
- **Zero-knowledge encrypted**: Bitwarden team members can't see your vault data, including data like URLs that other password managers don't encrypt, or your master password.

Clients

Password Manager offers client applications for most devices and many use-cases:

- **Web app**: The Password Manager web app is your home for vault administration and organization management. Get started today.
- **Browser extensions**: Password Manager browser extensions are perfectly suited for autofilling and seamlessly creating credentials to make surfing the web even easier. Get started today.
- **Mobile apps**: Password Manager mobile apps are built to help you securely take your credentials on the go. Get started today.
- **Desktop apps**: Password Manager desktop apps bring a full and elegant vault experience natively to your desktop. Get started today.
- **CLI**: The Password Manager command-line interface (CLI) is a powerful, fully-featured tool for accessing and managing your vault, and is well-positioned to help in automated or development workflows. Get started today.